REMARKS

I. Introduction

In response to the Office Action dated May 31, 2007, claims 1 and 16 have been amended. Claims 1-30 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Telephone Interview Summary

Record is made of a telephone interview between Applicants' attorney and Examiner Yalew that occurred on May 30, 2007. The prior art rejections and claims were discussed, but no agreement was reached on allowable claims.

III. Prior Art Rejections

A. The Office Action Rejections

On pages 2-5 of the Office Action, claims 1-30 were rejected under 35 U.S.C. §103(a) as being unpatentable over Fleishman (U.S. Patent No. 4,232,313) in view of Dube (U.S. Patent No. 7,177,426).

Applicants' attorney respectfully traverses these rejections.

B. The Applicants' Independent Claims

Independent claims 1 and 16 are generally directed to data set comparison and net change processing by a computer. Independent claim 1 is representative and recites a method for processing data comprising: receiving a plurality of fixed coordinates, each independently representing a location of an item; utilizing a cryptographic algorithm to encrypt the plurality of fixed coordinates forming a processed data; and comparing the processed data to at least a portion of secondary data that comprises one or more fixed coordinates to determine whether a match exists.

C. The Fleishman Reference

Fleishman describes a method and apparatus for the tactical navigation and communication of a community of aircraft. Each of the aircraft in the community is provided with an inertial navigation system capable of providing accurate short term navigational information and a time synchronized ranging system capable of providing accurate long term navigational information. One of the aircraft is designated as the airborne control unit and establishes a relative grid coordinate system within which the community of aircraft operate. The origin of the relative grid is established by the airborne control unit. When stationary ground time synchronized ranging system units are present, highly accurate georeferenced information may be supplied to the airborne control unit by operation of its time synchronized ranging system. When such ground units are not present, accurate georeferenced information may be obtained by the airborne controller from navigational systems such as satellite, Loran or Omega systems. The remaining or "user" aircraft in the community determine their position in the relative grid by interrogating the airborne control unit with their time synchronized ranging systems. A Kalman filter technique is employed to update the short term navigational information derived from the inertial navigation system in each user aircraft with the long term navigational information obtained from the time synchronized ranging system, so that the highly accurate georeferenced navigational information from the airborne control unit is provided to each member of the community of user aircraft. Novel computer programming permits each aircraft in the community to derive navigational information having the best characteristics of navigational information available from several sources, so that very accurate navigation in the area defined by the relative grid is made possible. The system of the invention may also perform communication and identification functions for the members of the tactical community.

D. The Dube Reference

Dube describes an invention for electronic file protection using location and other entropy factors. Environment information regarding a computer is obtained, wherein the environment information includes data concerning an operating environment of the computer. Based on the environment information, an encryption key is generated and an electronic file is encrypted using the encryption key. A decryption key can also be created based on environment information, wherein the decryption key can be utilized to decrypt the electronic file. In addition, the environment information can include location information of the computer, drive information regarding a drive wherein the electronic file will be stored, and time information specifying access duration.

E. The Applicants' Invention is Patentable Over the References

The Applicants' claimed invention is patentable over the references, because the claims contain limitations not taught by the reference. Specifically, Applicants' invention is designed to use a cryptographic algorithm to identify, disclose and compare multiple sets of coordinates representing the location of a particular item in a secure and confidential manner. These essential features are not taught or suggested by the references.

The Office Action, on the other hand, asserts that Fleishman describes "receiving a plurality of fixed coordinates that represent a location of an item," at col. 40, lines 60-66, which is reproduced below:

> Fleishman: col. 40, lines 60-66
>
> The control aircraft 502 may be equipped to receive highly accurate georeferenced navigational information from a variety of sources, such as a satellite system 503, ground TSRS stations 504 and TSRS-equipped bouys 505. The control aircraft 502 may then elect to direct an attack on the target 501 by transmitting the relative grid coordinates of the target to various "strike" aircraft 506, previously positioned ground artillery 507, or an off-shore missile ship 508.

The Office Action admits that Fleishman does not disclose "utilizing a cryptographic algorithm to process the plurality of fixed coordinates forming a processed data," and "comparing the processed data to at least a portion of secondary data."

Nonetheless, the Office Action asserts that Dube describes "utilizing a cryptographic algorithm to process the plurality of fixed coordinates forming a processed data," and "comparing the processed data to at least a portion of secondary data," at col. 5, lines 14-24, Fig. 13 Step 1310 and Fig. 15, step 1510, which are reproduced below:

> Dube: col. 5, lines 14-24 (actually, lines 8-24)
>
> Broadly speaking, the present invention fills these needs by providing electronic file protection using location and other entropy factors. In one embodiment, a method for protecting electronic files is disclosed. Environment information regarding a computer is obtained, wherein the environment information includes data concerning the operating environment of the computer. Based on the environment information, an encryption key is generated and an electronic file is encrypted using the encryption key. A decryption key can also be created based on environment information, wherein the decryption key can be utilized to decrypt the electronic file. In addition, the environment information can include location information of the computer, drive information regarding a drive wherein the electronic file will be stored, and time information specifying access duration.

Dube: Fig. 13

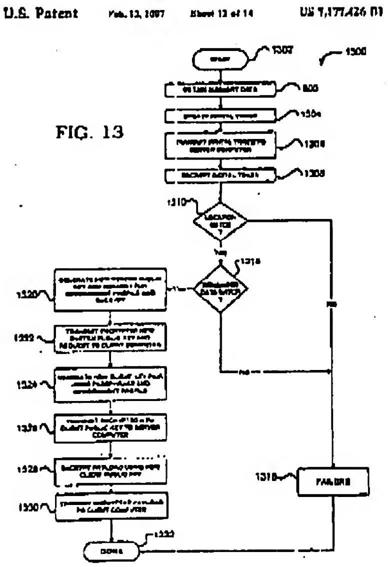

FIG. 13

Dube: col. 17, line 42 – col. 18, line 32

FIG. 13 is a flowchart showing a method 1300 for protecting electronic files based on location, in accordance with an embodiment of the present invention. In an initial operation 1302, preprocess operations are performed. Preprocess operations include establishing a connection with a remote server computer, commencing the transaction application, and other preprocess operations that will be apparent to those skilled in the art.

In operation 800, summary data including GPS entropy data is obtained.

Summary data is obtained as discussed previously with respect to method 800 of FIG. 8. The obtained summary data is stored in temporary memory 624 and the client random number stack 612 and the client delay stack 614 are updated as discussed above.

A digital token is created in operation 1304. The User Card uses the system default public key in conjunction with the client private key to encrypt the summary data stored in the temporary memory into a digital token. For example, the summary data can include the GPS time and date, the calculated geophysical location, the selected previously stored delay number, the selected previously stored random number, the client ID, and the receiver ID. It should be bome in mind that the digital token is not required to include all the information stored in temporary memory. In some embodiments, some amount of summary information less than all the information shown in the temporary memory mentioned above is encrypted into the digital token.

The digital token is transmitted to the server computer in operation 1306. Upon receipt, the server computer decrypts the digital token, in operation 1308. The server computer decrypts the digital token using the system default private key. The server computer then compares the summary data included in the digital token to the data included in the user profile.

A decision is then made as to whether the GPS geophysical location data included in the digital token matches the GPS geophysical location data included in the user profile, in operation 1310. If the GPS geophysical location data included in the digital token matches the GPS geophysical location data included in the user profile, the method 1300 continues with operation 1318. Otherwise, the method 1300 continues with an authentication failure operation 1316. In the authentication failure operation 1316, access to the server computer is denied and the system administrator is notified to take any subsequent actions that have been instituted by the organization.

In operation 1318, a decision is made as to whether the remainder of the summary data included in the digital token matches the data included in user's profile. For example, the client ID and receiver ID can be validated. If the remainder of the summary data included in the digital token matches the data included in user's profile, the method 1300 continues with operation 1320. Otherwise, the method 1300 branches to the authentication failure operation 1316.

A new system public key is generated and both the new system public key and a request for the environment profile are encrypted, in operation 1320.

Dube: Fig. 15

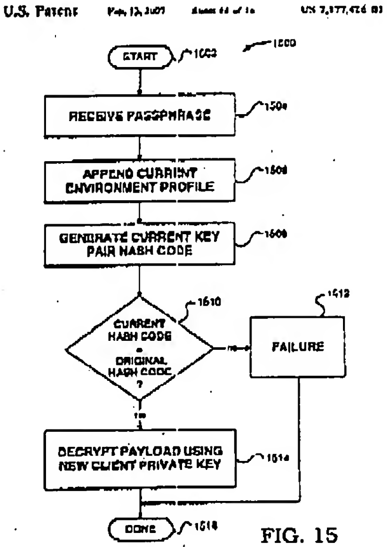
U.S. Patent
START
1502
1500
RECEIVE PASSPHRASE
1504
APPEND CURRENT ENVIRONMENT PROFILE
1506
GENERATE CURRENT KEY PAIR HASH CODE
1508
CURRENT HASH CODE = ORIGINAL HASH CODE ?
1510
no
FAILURE
1512
yes
DECRYPT PAYLOAD USING NEW CLIENT PRIVATE KEY
1514
DONE
1516

FIG. 15

Dube: col. 19, line 18 – col. 20, line 13

FIG. 15 is a flowchart showing a method 1500 for accessing an encrypted data file, in accordance with an embodiment of the present invention. In an initial operation 1502, preprocess operations are performed. Preprocess operations can include authorizing a transaction to receive the encrypted data file, generating an

> environment profile, receiving the encrypted data file, and other preprocess operations that will be apparent to those skilled in the art.
>
> In operation 1504, the user's passphrase is received. The user is prompted to either enter their passphrase or PIN number. If biometric access is being used, the user is prompted to verify their identity through a biometric access device. A summary of the user's biometric characteristics can then be created. In some embodiments, the passphrase or biometric summary can be compared to a stored user profile to authenticate the user.
>
> The current environment profile is then appended to the passphrase, in operation 1506. As mentioned above, the environment profile is based on the operating environment of the client computer and can include geo-location, drive ID(s), electronic address assignments, time ranges, and other environmental variables that can be obtained or measured. These environmental variables are then hashed to created a current environment profile that represents the current operating environment of the client computer.
>
> In operation 1508, the passphrase and the appended current environment profile are hashed to create a current key hash code. As mentioned above, embodiments of the present invention process the passphrase and the appended environment profile to generate the new client public and private key pair, which is used for file encryption. In addition, during the new client key pair creation, the hash code based on the new client public and private key pair and environment profile can be saved. This saved original key pair hash code can be used for verification.
>
> **A decision can then be made as to whether the current key pair hash code matches the original key pair hash code, in operation 1510.** If the current key pair hash code does not match the original key pair hash code, the method 1500 fails in operation 1512. Hence, the file access can fail because of a change in the operating environment as well as by entering the wrong passphrase. If the current key pair hash code matches the original key pair hash code, the method 1500 continues with a decrypting operation 1514.
>
> In decrypting operation 1514, the encrypted payload data file is decrypted using the new client private key. Hence, if the expected operating environment is maintained at the time of file access, the new client private key is used to decrypt the data file. In a further embodiment of the present invention, the passphrase and appended current environment profile are used to generate another new client private key. This client private key is then used to decrypt the payload data. However, the movement, removal, or re-arrangement of one or more environment variables will cause the composition of the environment profile to change, thereby creating an incorrect private key for use in the decryption process. An invalid key, of course, will be unable to decrypt the file. Hence, as mentioned above, the embodiments of the present invention allow a data file, System Card, or User Card to lockup data upon the change of any one or more devices from their original prescribed configuration of geo-physical and electronic addresses.

Finally, the Office Action asserts that it would have been obvious to one of ordinary skill in the art to modify the method for processing data of Fleishman with the encryption of Dube because the encryption protects sensitive data.

Applicants' attorney disagrees with this analysis.

The above portions of Fleishman merely describe a control aircraft directing an attack on a target by transmitting the relative grid coordinates of the target to various strike aircraft, artillery or ships. However, while it receives multiple signals in order to fix its location, it generates only one set of coordinates for its target, but it does not receive a plurality of fixed coordinates, each independently representing a location of an item.

Moreover, the above portions of Dube merely describe providing electronic file protection using a location and other entropy factors to generate an encryption key for encrypting the file. However, while it generates the encryption key from a single location value, it does not utilize a cryptographic algorithm to encrypt a plurality of fixed coordinates and then compare the encrypted plurality of fixed coordinates to some other data to determine whether a match exists.

Thus, even when combined, the Fleishman and Dube references would not teach or suggest the limitations of Applicants' independent claims. Indeed, neither Fleishman nor Dube operate in the same context as Applicants' claims, namely using a cryptographic algorithm to identify, disclose and compare multiple sets of coordinates, each set of coordinates independently representing the location of a particular item, in a secure and confidential manner.

Moreover, the Fleishman and Dube references cannot be combined in the manner suggested by the Office Action, since they operate in such disparate fields of technology.

Thus, Applicants' attorney submits that independent claims 1, 18, 34 and 51 are allowable over Fleishman and Dube. Further, dependent claims 2-17, 19-33, 35-50 and 52-66 are submitted to be allowable over Fleishman and Dube in the same manner, because they are dependent on independent claims 1, 18, 34 and 51, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-17, 19-33, 35-50 and 52-66 recite additional novel elements not shown by Fleishman and Dube.

IV. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited.

Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: August 31, 2007

By:______________________
Name: George H. Gates
Reg. No.: 33,500

GHG/

G&C 30571.300-US-01